Solution Overview

Cisco Security Management Suite

The Cisco® Security Management Suite is a framework of next-generation security management tools designed for the operational management and policy administration of the Cisco Self-Defending Network. This suite of integrated applications simplifies the management process by automating tasks associated with the functional areas of security management: configuration, monitoring, analysis, mitigation, identity, and auditing. The result is an increased level of security assurance, better organizational productivity, and lower overall TCO.

The primary components of the Cisco Security Management Suite include the Cisco Security Manager and the Cisco Security Monitoring, Analysis, and Response System (MARS).

CHALLENGE

The network has become a vital component of the organizational business process, and administrators are faced with the challenge of securing this control plane. As a result, we have seen the convergence and integration of security features, services, and capabilities into the network fabric itself. While this can be an efficient method to secure an enterprise network, it also presents organizations with some unique management challenges:

- Integration of network and security IT operations teams creating uncertainty over ownership of tasks and resources
- Complexity of business-level security policies being translated into actionable rules for the network to follow
- An overwhelming amount of information and security data, making it difficult to identify security threats
- The ability to track users accessing the corporate resource and determining who can do what on the network and when

A complete and integrated management solution is needed, one that can simplify the operational processes associated with these challenges.

SOLUTION

The Cisco Security Management Suite is a framework of next-generation tools that addresses the security management challenges of today’s converged networks. Functionally, these tools provide a framework for configuration, monitoring and analysis, and threat mitigation. The products that make up this suite are:

- Cisco Security Manager
- Cisco Security Monitoring, Analysis, and Response System (MARS)

Figure 1. Cisco Security Management Suite—The Integrated Solution for Managing the Self-Defending Network

Cisco Security Manager
Configuration • Provisioning
Cisco Security Management Suite
Monitoring • Analysis • Mitigation
Cisco Security MARS

Cisco Security Manager is a powerful but easy-to-use solution for configuring firewall, VPN, and intrusion prevention system (IPS) policies on Cisco security firewalls, routers, and appliances (Figure 2). To deal with the complexity of different security devices, operating systems, and configuration interfaces, Cisco Security Manager has been designed to act as a layer of abstraction. The result is an application with usability enhancements that deliver a superior look and feel to simplify the process of scalable policy definition and deployment (Figure 3). For example, if a network or security administrator wants to implement a policy of limited instant-messaging traffic during business hours, they can do so in a series of simple clicks. The user experience is the same regardless of the actual security device type that is enforcing the rule—whether it is a Cisco PIX® firewall, a Cisco IOS® Software-based integrated services router, a Cisco ASA adaptive security appliance, or a Cisco Catalyst® switch services module. Cisco Security Manager helps administrators reduce user error and maintain consistent policies across the secure network infrastructure.

Figure 2. Cisco Security Manager Map View

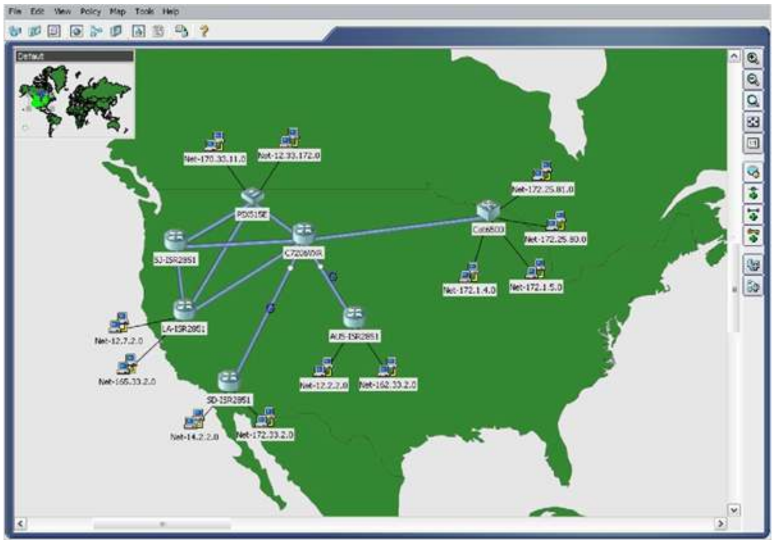
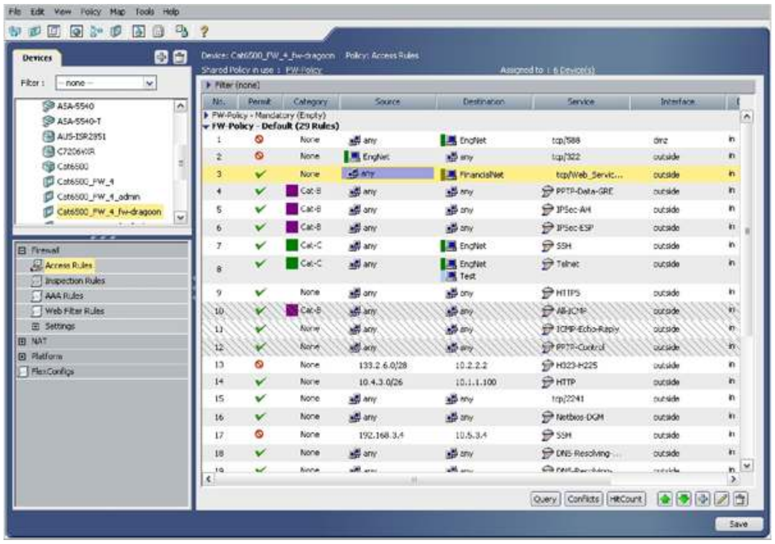


Figure 3. Cisco Security Manager Policy Rule Table



Device: Cat6500_FW_4_fw-dragoon Policy: Access Rules
Shared Policy in use : FW-Policy Assigned to : 6 Device(s)

Filter (none)

FW-Policy - Mandatory (Empty)

FW-Policy - Default (29 Rules)

No.	Permit	Category	Source	Destination	Service	Interface	
1	⊘	None	any	EngNet	tcp/588	dmz	in
2	⊘	None	EngNet	any	tcp/322	outside	in
3	✓	None	any	FinancialNet	tcp/Web_Servic...	outside	in
4	✓	Cat-B	any	any	PPTP-Data-GRE	outside	in
5	✓	Cat-B	any	any	IPSec-AH	outside	in
6	✓	Cat-B	any	any	IPSec-ESP	outside	in
7	✓	Cat-C	any	EngNet	SSH	outside	in
8	✓	Cat-C	any	EngNet Test	Telnet	outside	in
9	✓	None	any	any	HTTPS	outside	in
10	✓	Cat-B	any	any	All-ICMP	outside	in
11	✓	None	any	any	ICMP-Echo-Reply	outside	in
12	✓	None	any	any	PPTP-Control	outside	in
13	⊘	None	133.2.6.0/28	10.2.2.2	H323-H225	outside	in
14	✓	None	10.4.3.0/26	10.1.1.100	HTTP	outside	in
15	✓	None	any	any	tcp/2241	outside	in
16	✓	None	any	any	Netbios-DGM	outside	in
17	⊘	None	192.168.3.4	10.5.3.4	SSH	outside	in
18	✓	None	any	any	DNS-Resolving-...	outside	in
19	✓	None	any	any	DNS-Resolving-...	outside	in

The second component of the Cisco Security Management Suite is Cisco Security MARS, an appliance-based, all-inclusive solution that provides insight and control of the existing security deployment. This appliance allows network and security administrators to identify, manage, and counter security threats. By using the existing network and security infrastructure, Cisco Security MARS can monitor security events and information from a wide variety of sources, including third-party devices and hosts. By using a best-of-breed correlation engine, Cisco Security MARS can not only identify anomalous behavior and security threats, but can also recommend precision removal of those elements, leading to rapid threat mitigation. In addition, the Cisco Security MARS appliance can use the vast amounts of information collected for forensics analysis and compliance reporting.

These products are built upon an architecture that facilitates integration with other security management tools for even greater value. The Cisco Secure Access Control Server provides identity-based services that provide centralized control for role-based access to the management applications. This allows administrators to ensure enforcement of assigned policies on user access rights, privileges, and command controls. With Cisco Secure

ACS acting as the policy control point with authentication, authorization, and accounting (AAA) services, network and security administrators can help enforce the rules of who is allowed onto the network, what they are allowed to access, and when.

Together, these applications provide the core capabilities for managing a Cisco security network. The products within this suite might not directly address every challenge facing a network. Examples of this might include antivirus software to protect servers and hosts or vulnerability assessment tools. To address these needs, Cisco Systems® looks to other products in its broad portfolio and also engages in a comprehensive partner strategy that allows customers to truly take advantage of best-of-breed products. By providing this integration, the Cisco Security Management Suite delivers a next-generation solution for managing today’s security networks.

INTEGRATED ARCHITECTURE

The tools within the Cisco Security Management Suite are built upon a framework that facilitates communication between the components. This integration enables network and security administrators to derive additional value from implementing the complete solution.

For example, when Cisco Security MARS is monitoring the network and a specific security incident is detected, the appliance has the ability to correlate that incident to the policy rule that has been violated within Cisco Security Manager to create that event. By providing a simple Web linkage, an administrator is able to quickly drill down from event notification to identification, along with specifics about the precise network behavior that caused the incident. This level of integration adds tremendous value in terms of facilitating workflow within an organizations management group.

Another example is the linkage between Cisco Secure ACS with the other management applications in the suite. Using the AAA services as a policy control engine, administrators can enforce role-based access control (RBAC) for Cisco Security Manager. Depending on a specific user’s privileges, they may be able to only define policy, or perhaps deploy policy, or perhaps even only view configurations on a specific set of devices. This level of control is especially important when working with a powerful security configuration application such as Cisco Security Manager.

Cisco’s strategy is to address the security management challenges and pain points from a business process perspective, not from an individual point product perspective. These areas of value-added integration will continue to evolve along with the Cisco Security Management Suite, making the solution the ideal method to manage Cisco Self-Defending Network.

BUSINESS BENEFITS

With a powerful set of applications, an integrated architecture, and a comprehensive partnering strategy, the Cisco Security Management Suite is positioned to provide organizations with a best-of-breed management solution for their security networks. With tools that automate and simplify operational tasks, administrators can derive value from:

- **Policy consistency and security assurance**—Cisco Security Manager allows you to deploy consistent security policies across thousands of security devices in a short span of time.
- **Rapid threat mitigation for improved company network uptime**—Cisco Security MARS allows organizations to quickly identify and respond to network and security threats such as worms and viruses, preventing widespread outbreaks and significant downtime.
- **Better control of and access to security information for forensics analysis and reporting**—The applications in the Cisco Security Management Suite can collect information that is instrumental for organizational compliance reporting.
- **Accounting and tracking of user network access and authorization**—Cisco Secure ACS provides a central policy engine to control user access and privilege levels for network access.

By providing this level of integration, the Cisco Security Management Suite delivers increased security, better organizational productivity, and lower overall TCO.

SUPPORTING SOLUTIONS, PRODUCTS, PARTNERS, OR SERVICE OFFERINGS

Supporting solutions, products, and partner offerings for the Cisco Security Management Suite include:

- The Cisco Self-Defending Network
- Cisco Network Admission Control
- Cisco Incident Control System

WHY CISCO

With its powerful applications and integrated architecture, Cisco can provide the broadest range of security solutions for enterprise customers. Now with a single solution, administrators can confidently configure systems, monitor events, analyze and respond to threats, and manage network users throughout their entire integrated security infrastructure. The Cisco Security Management Suite provides the following benefits:

- Improved return on investment through enhanced security, based on intelligent tools that enable quick and easy detection, location, and mitigation of attacks
- Lowered total cost of ownership due to a consistent application of security policies across devices, and matching those policies to administrative workflows
- Increased IT productivity based on automation of mass configurations of security policies, bulk firmware upgrades, and ongoing management of remote firewalls
- More simple, elegant system designs that enable better management of hundreds of thousands of security devices
- Integrated system usage across the enterprise based on an easy-to-use Web-based GUI that allows staff to work effectively with a wide range of devices
- Better cost control due to decreased disruptions as a result of less user error

FOR MORE INFORMATION

For more information about the Cisco Security Management Suite, visit http://www.cisco.com/go/security_management or contact your local account representative.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA

C02-60008-00 01.06